AU/ACSC/PARTLOW/AY10

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

SPACE SYSTEM VULNERABILITIES AND DEFENSES

by

Raymond G. Partlow, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Maj Mia Walsh

Maxwell Air Force Base, Alabama

March 2010

Short Research Paper
Maj Raymond Partlow (16-9835)

Most modern nations are dependent to some degree on space but the U.S. is perhaps the world's most space dependent nation.[1] Space assets are involved in most daily activities such as withdrawing money at an ATM machine, making a phone call, or watching television.[2] While the use of space arguably increases the quality of life in space faring nations as well as large portions of the rest of the world, there is also a downside to space use. As nations, especially the U.S., become more dependent upon space they are also more vulnerable to attack by an enemy. The following discussion will begin by outlining how nations depend on space, explore some simple scenarios if enemies denied the use of space, discuss the vulnerabilities of space systems, then conclude with some defensive concepts.

Use of space is embedded into the daily lives of most Americans to the point that they may not even realize how often they are using space. Most Americans probably think of the Global Positioning System (GPS) when they think of using space. They use GPS receivers in their cars to find their way to places unfamiliar to them. However, they also frequently use GPS in the form of timing information when removing money from an ATM or making a phone call, although most of them probably don't realize it. Many Americans' television programming is also delivered to their homes via satellites. Even if the source of their TV signal is an antenna or cable TV, the program they are watching was likely transmitted via satellite at some point in its path to their home. The U.S. government is also very dependent on space, particularly the U.S. military.

U.S. military uses of space include beyond line of sight communications, GPS navigation and weapons guidance, intelligence and surveillance, and missile warning functions. Denying these capabilities to the military during planning or operations would have a crippling effect. Imagine the U.S. Army trying to navigate in a featureless desert without the benefit of GPS or

imagine the Air Operations Center trying to control a strike package without beyond line of sight communications. Such limitations would make successful U.S. military operations very difficult if not impossible. An attack on space assets could also seriously hurt America economically. Financial institutions could potentially have great difficulty exchanging information with one another while the American civilian population may be reduced to mass panic if people are unable to get access to their money. At the very least, the American public would likely consider it a major inconvenience if national television programming were interrupted. Unfortunately, attacking these capabilities is within the means of a nation (or even a terrorist group) with reasonable technical proficiency.

A space system in its simplest form is made up of ground stations and one or two satellites. The ground stations are used to control the satellites as well as send information to and receive information from the satellites. To be successful, an attack must interrupt the communication between the ground stations and the satellites. This can be accomplished in several ways, both kinetic and non-kinetic.

An example of a kinetic attack on a space system is a direct ascent Anti-Satellite (ASAT) weapon, such as that recently tested by China, which destroys a satellite on orbit. Another example is a bomb attack on a ground station in the system. Either kinetic attack will at least reduce the functionality of the space system if it does not outright destroy it. However, there are non-kinetic attack methods which are just as effective. These include jamming uplinks and downlinks, dazzling or partially blinding sensors with lasers, and attacks with high powered microwaves.[3]

As previously mentioned, satellites communicate with ground stations for various purposes. Information sent from the ground station to the satellite is known as an uplink while

information sent from the satellite to the ground station is known as a downlink.[4] These links are composed of data encoded on a radio frequency (RF) carrier wave and are vulnerable to being jammed in the same manner as any signal carried in this way. All that must be done is to broadcast another signal on the same frequency, but at much higher power than the signal to be jammed.[5] Jamming either the uplink or downlink effectively removes the satellite from the system. This effect is only achieved as long as the satellite or ground receiver is in view of the jamming transmitter.

Intelligence/reconnaissance satellites with optical or infrared (IR) sensors provide a vulnerability to attack in the form of the imaging sensor. A high intensity laser directed at the sensor may result in either dazzling the sensor or partially blinding it. Dazzling refers to temporarily preventing the sensor from properly imaging the ground in an effect similar to shining a bright flashlight into someone's eyes.[6] However, once the laser passes out of view of the satellite's sensor, the satellite is again able to see the earth and take proper images. Although the effect is temporary, it is possible for an adversary to prevent a satellite from taking images of a specific area. In the event a high powered laser is powerful enough and allowed to linger on the satellite's imaging sensor long enough, the laser can successfully partially blind the sensor.[7] This effect is similar to burning the retina in a human eye. In this case, once the laser passes out of view of the satellite's sensor, the sensor is still unable to image the earth. The sensor is now permanently damaged and the satellite may be useless to fulfill its intended function of intelligence/reconnaissance.

One final non-kinetic means of attacking a satellite is through High Powered Microwaves (HPM). This attack uses very intense microwave radiation to interfere with the electronic circuitry and computers on the satellite.[8] Using HPM from the earth's surface to damage a

satellite is difficult because of the vast distance involved and the attenuating effects of earth's atmosphere on microwave radiation.[9] Therefore, an attack of this type is most likely to originate from another spacecraft, either in orbit with the satellite being attacked or on a suborbital trajectory that puts it in view of the satellite being attacked but above the earth's atmosphere.[10] The effects of HPM attacks are generally unpredictable and range from causing system restarts to permanent damage of electronic components.

There are several technical issues that must be solved when attacking any satellite on orbit. In the event of a direct ascent kinetic weapon, the weapon must physically contact the satellite in question. In the case of a non-kinetic attack, the satellite must be tracked and the jammer, laser, or HPM must be aimed at the satellite as it is moving. While these do pose significant challenges, a country technologically advanced enough to create the weapon probably also has the ability to aim it.

Obviously, the most effective defense against all these forms of attack is for a nation to decrease its reliance on space. However, decreasing reliance on space tends to also decrease the quality of life for the nation's people and is therefore not desirable. A better approach is to devise a defense to protect the space systems so vital to a nation.

When attempting to counter a kinetic, direct ascent, anti-satellite weapon there is little to be done to protect the targeted satellite other than try to constantly maneuver it. Constant maneuvering would render the firing solution of the direct ascent weapon invalid. However, it also uses up valuable maneuvering fuel in the satellite and could reduce the life of the satellite below any period of time considered useful. Another potential tactic is to affect the terminal guidance of the anti-satellite weapon so that the weapon misses the targeted satellite, but this technology is still in the development phase, at least at the unclassified level. Therefore, there

really is no effective defense against this type of weapon, for now. On the other hand, there are currently defenses available against RF jamming, lasers, and HPM attacks.

Defenses against HPM attacks involve hardening the satellite electrically so that HPM cannot harm its sensitive electronics.[11] Such hardening does not involve great cost if it is incorporated in the early stages of the satellite's design.[12] However, it still increases cost, even if moderately, and this could prove unattractive for some business applications. A commercial service provider, such as DirecTV for example, attempts to make a profit by charging customers for the use of its satellite. Even a moderate increase in the developmental cost of the satellite may dramatically and adversely affect the company's profit margin. The service provider, DirecTV in this example, may decide the risk of their satellite being attacked is low compared to the cost of hardening against such an attack and forgo the increased cost. Therefore, it may be only the most critical satellites, such as intelligence and government communications systems, that will be hardened against HPM. This leaves a potential vulnerability in a nation's commercial sector that an adversary can exploit.

A satellites imaging optics can be protected from lasers by preventing the laser energy from entering those optics. This can be accomplished through the use of a filter or a fast acting shutter. A filter blocks light of a specific wavelength while allowing other wavelengths of light to pass into the satellite's optics. A major weakness of this system is that if the laser light is not in the wavelength the filter is designed to block, then the filter will be ineffective. Also, many lasers may operate in the wavelength of light that the satellite is trying to collect to build an image. In this case, blocking the laser energy also means blocking the useful light required by the satellite to perform its mission. A fast acting shutter, on the other hand, allows all light to pass into the imaging optics until the shutter is closed. In order for a shutter like this to be

effective it must first detect the laser energy and then close rapidly enough to prevent the laser from damaging the sensitive optics. Developing such a fast acting shutter is difficult because high powered laser energy does not require much time to cause permanent optical damage. However, even if the shutter can be developed and employed, closing off the optics to the laser also prevent the optics from gathering light to build the desired image, effectively rendering the satellite inoperative for a least a short period of time.

Perhaps the easiest attack to counter is jamming. Receivers on both the ground and satellite have been developed to detect signals through the interference of noise jamming and to ignore false signals produced by deceptive jamming techniques. However, as discussed in the next paragraph, anti-jam technology is typically developed once the jamming technology it is designed to counter is already in place. This technology is also expensive and may prove too costly for anyone other than government built and operated satellite systems.

The biggest problem with developing a defense against space system attacks is it is rarely possible to develop a defense against a specific method of attack until that method is actually employed. As an example, RF receivers exist that can detect a signal in a noise jamming environment and ignore false signals in a deceptive jamming environment. However, a marked increase in the power output of a noise jammer or a previously unknown deceptive technique may render current anti-jam receivers susceptible to jamming interference. The receivers can only be built to counter jamming that has already been observed and characterized or the developer's best guess at a future jamming technique. In other words, defenses are always playing catch up in that they are designed to counter a weapon which has likely already been deployed and is holding a space asset at risk. A nation must wait until it knows details about a particular weapon before it can devise a defense against it. Therefore, that nation is at a

disadvantage in protecting its space assets. Arguably, most nations developing space weapons are counting on this very fact to ensure their weapons are a credible threat. Therefore, a comprehensive defense against attacks on space assets must include concepts to react once a satellite is disabled.

In the event that an attack on a space system is successful, there are still ways to minimize the overall damage caused by the attack. Building redundancy into the space system will ensure even if part of the system is inoperative, the overall system can still function. As an example, the GPS constellation is composed of around 30 satellites.[13] The satellites work together as a system to provide accurate time and position information. The loss of any single satellite will potentially degrade the accuracy of the overall system, but the system will continue to provide time and position information. The more satellites rendered inoperative, the greater the degradation of the system's accuracy. However, there is no single satellite whose loss will disable the system.

Another concept to minimize the effects of a successful attack on a space system is rapid replenishment.[14] This is an overall concept comprising two smaller concepts: rapid launch of stored spares and repositioning of on orbit spares. The idea of rapid launch of stored spare assets states that a supply of launch ready satellites is maintained in such a condition they can be launched and put into operation relatively quickly. In this case, relatively quickly refers to hours or days rather than weeks or years.[15] In this way, damaged or destroyed space assets on orbit can be quickly replaced. Of course, for this to truly be effective there must be a supply of satellites likely to be attacked waiting in standby or the satellites must be able to be built in a matter of days. Storage costs for these standby satellites will likely be very high. Additionally, a launch vehicle capable of rapid response launching does not yet exist. As for rapidly building a satellite,

this has been accomplished for simple satellites as an academic exercise, but completing construction of a national asset in a short time will be difficult if not impossible because of its complexity.[16] So, while this concept may be possible in the future, it is not yet viable. Another option for rapid replenishment however, is the idea of having spare satellites maintained on orbit. In that case, when a satellite is damaged or destroyed, the orbiting spare is rapidly moved into position to take over from the attacked satellite. The current GPS constellation uses an approach similar to this.[17]

As nations increase the quality of life for their people and the effectiveness of their military by using space systems, they also increase their vulnerability to an enemy. Removing a space system from service, even temporarily, can have devastating effects on a nation's military capabilities and even affect its economy. There are many ways to attack a space system including kinetic direct assent ASAT systems as well as non-kinetic lasers, jammers, and High Powered Microwaves. All of these can have dramatic temporary effects and possibly even crippling permanent effects. Defenses, or in some cases defensive concepts, against these attacks exist. However, these defensive measures increase cost of the overall space system. In some cases, the cost is minimal while in other cases the cost is very high. For a government system, the increased cost of defense will be absorbed by the government. For a commercial business however, this increased cost can be the difference between a viable and an unsustainable business. Therefore, a nation's space assets may only be protected if those assets are government operated. However, all nations including the U.S. must weigh the cost of space asset defense against the risk of attack on those assets by the nation's enemies.

[1] Johnson-Freese, *Space as a Strategic Asset*, 1.
[2] Ibid.

[3] Wright, Grego, and Gronlund, *The Physics of Space Security*, 118-132.
[4] Ibid, 118.
[5] Ibid.
[6] Ibid, 125.
[7] Ibid, 128.
[8] Ibid, 131.
[9] Ibid.
[10] Ibid.
[11] Ibid, 133.
[12] Ibid.
[13] Mehuron, *2009 Space Almanac*, 63.
[14] USJFCOM, *the Joint Operating Environment 2010*, 37.
[15] ACSC, *AU-18 Space Primer*, 270.
[16] ACSC, Operational Space Elective.
[17] ACSC, *AU-18 Space Primer*, 218.

Bibliography

Air Command and Staff College (ACSC). *AU-18 Space Primer*. Air University Press, 2009.

Johnson-Freese, Joan. *Space as a Strategic Asset*. Columbia University Press, 2007.

Mehuron, Tamar. *2009 Space Almanac, The U.S. Military Space Operations in Facts and Figures*. Compiled by Tamar Mehuron for Air Force Magazine, 2009.

United States Joint Forces Command (USJFCOM). "the Joint Operating Environment 2010." USJFCOM, 2010.

Wright, David, Grego, Laura, and Gronlund, Lisbeth. *The Physics of Space Security*. Wright, Grego, and Gronlund, 2005.